August 1, 2019

Beryl Lipton
MUCK ROCK
Email: 69523-00112558@requests.muckrok.com

RE: Public Records Request
LVMPD PIO Request No. F190617-01

Dear Ms. Lipton:

This correspondence is in response to your public records request received by the Las Vegas Metropolitan Police Department (LVMPD) Office of Public Information on or about June 17, 2019. You are requesting the following information:

- Agreements: contracts (including non-disclosure agreements), licensing agreements, nondisclosure agreements
- Bid records: Requests For Proposal (or equivalent calls for bids), sole source or limited source justification and approval documentation, documentation of selection, and other materials generated in the consideration and selection of the technology in question
- Company relations and communications: records related to meetings or follow-up actions with any vendors, companies, or other private entities marketing face recognition to this agency for immigration, intelligence, law enforcement, or other use.
- Financial records: purchase orders, invoices, and other memoranda and documentation.
- Marketing records: All marketing materials - unsolicited, requested, or otherwise - acquired from vendors of face recognition technology
- Policy records: any policy directives, guidance documents, memoranda, training materials, or similar records governing the use of face recognition technology for immigration, law enforcement, or other purposes.
- Training records: training material governing the use, sharing, or access to any related data related to or collected by the face recognition software/technology, including the legal standard that is required before using the technology

- Use and function records: Materials that describe the function of the software considered or in use by this agency, including emails, handouts, PowerPoint presentations, advertisements, or specification documents.

The records responsive to your request that are not confidential by law are enclosed herewith.

There is a training video that is withheld as being proprietary and containing law enforcement techniques. *See, Donrey of Nevada, Inc. v. Bradshaw*, 106 Nev. 630, 798 P.2d 144 (1990) (adopting the law enforcement privilege from the federal Freedom of Information Act, which includes materials concerning law enforcement techniques and tactics); 18 U.S.C. §2512; NRS 332.061 (Proprietary information is not public information and is confidential); NRS 333.020(5) (Proprietary information defined); NRS 600A.030(5)(Trade secret defined); 5 U.S.C. §522(b)(3),(b)(4),(b)(7)(C) and (7)(E).

There are a few emails enclosed that were reasonably easy to locate. However, to conduct a comprehensive search and review of department-wide emails to identify any other emails that may be responsive is intrusive and would disrupt the Department's core functions. The Nevada Supreme Court has previously considered LVMPD's burdensome argument. *See LVMPD v. Blackjack Bonding*, 343 P.3d 608, 614 (2015). In *Blackjack*, however, LVMPD's burdensome argument involved the costs associated with production. The Supreme Court determined that the district court had mitigated any burdens because it ordered Blackjack to pay the costs associated with the production of the requested documents pursuant to NRS 239.052. *Id.* In addition to the financial burden LVMPD would incur in producing the requested records, discussed *infra*, the burden to search and review the records at issue will take significant time to accomplish.

Other courts have considered whether requests are too burdensome to produce prior to requiring production. *See Lunney v. State*, 418 P.3d 943, 954 (Ct. App. Ariz. 2017) (recognizing that the agency was not required to respond to the burdensome request); *Shehadeh v. Madigan*, 996 N.E.2d 1243, 1249 (Ill. App. Ct. 2013) (holding that the Attorney General satisfied its burden by explaining that its staff members would have to go through all of the 9,200 potentially responsive documents by hand); *Beckett v. Serpas*, 112 So.3d 348, 353 (La. App. Ct. 2013) (determining that segregating 10 years worth of files is unreasonably burdensome).

California courts recognize that an agency may legitimately raise an objection that a request is overbroad or unduly burdensome. *Community Youth Athletic Ctr. v. City of Nat'l City*, 164 Cal.Rptr.3d 644, 676, 220 Cal.App.4th 1385, 1425 (2013). An agency is obliged to comply so long as the record can be located with reasonable effort. *Id.* Such reasonable efforts do not require that agencies undertake extraordinarily extensive or intrusive searches, and in general, the scope of an agency's search for public records need only be reasonably calculated to locate responsive documents. *City of San Jose v. Superior Court*, 214 Cal.Rptr.3d 274, 288, 389 P.3d 848, 860 (2017).

To determine if producing documents "poses an unreasonable administrative burden," courts consider whether the general presumption in favor of disclosure is overcome by: "(1) the resources and time it will take to locate, compile, and redact the requested materials; (2) the volume of materials requested; and, (3) the extent to which compliance with the request will disrupt the agency's ability to perform its core functions." *Lunney*, 418 P.3d at 954.

Here, it would be burdensome to conduct a department-wide search of emails.

Should you have any questions or concerns, feel free to contact me.

Sincerely,

JOSEPH LOMBARDO, SHERIFF

By: _____
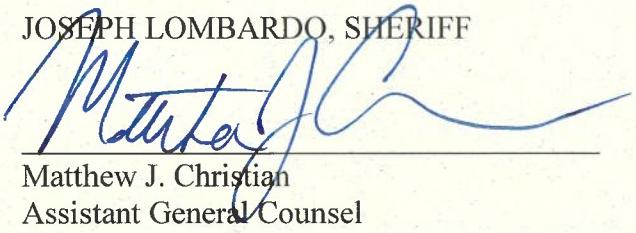
Matthew J. Christian
Assistant General Counsel

MJC:sa
Enclosures

5/206.19   FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons.

The LVMPD has established the capability to conduct facial recognition searches in support of law enforcement activities. This capability is primarily available through the facial recognition program, which is managed by the Technical Operations Section (Tech Ops).

PURPOSE

This policy provides LVMPD personnel with guidance and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a facial recognition program. This policy will ensure that all facial recognition searches are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals. Further, this policy will delineate the manner in which requests for facial recognition information is received, processed, catalogued, and responded to.

This policy assists LVMPD personnel in:
1. Increasing public safety and improving state, local, tribal, territorial, and national security.
2. Minimizing the threat and risk of injury to specific individuals.
3. Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
4. Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
5. Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
6. Making the most effective use of public resources allocated to public safety entities.

GENERAL USE

All deployments of facial recognition must be for official use for a law enforcement purpose only. A request for facial recognition analysis to Tech Ops will only be for official investigations that have a criminal predicate or an articulated public safety concern. The following are the authorized uses of facial recognition applications:
1. A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
2. An active or ongoing criminal or homeland security investigation.
3. To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.
4. To assist in the identification of a person who lacks capacity or is otherwise unable to identify himself (such as an incapacitated, deceased, or otherwise at-risk person).
5. To investigate or corroborate tips and leads.
6. For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.
7. To assist in the identification of potential witnesses or victims of violent crime.
8. To support law enforcement in critical incident responses.

This policy was also established to ensure that all images are lawfully obtained, including facial recognition probe images obtained or received, accessed, used, disseminated, retained, and purged according to LVMPD record retention policies. This policy applies to:
1. Images contained in a known identity face image repository and its related identifying information.
2. The facial recognition search process.

3. Any results from facial recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the LVMPD.
4. Lawfully obtained probe images of unknown suspects that have been added to unsolved image files pursuant to authorized criminal investigations.

FACIAL RECOGNITION SEARCHES

Facial recognition searches may only be performed by persons who have completed training and only during the course of lawful duties, in furtherance of a valid law enforcement purpose and in accordance with this policy. Valid law enforcement purposes include but are not limited to the following activities:

1. For persons who are detained for offenses that warrant arrest or citation.
2. For persons who are subject to lawful identification requirements and are lacking positive identification in the field.
3. For a person who an officer reasonably believes is concealing his true identity and has a reasonable suspicion the individual has committed a crime other than concealing his identity.
4. For persons who lack capacity or are otherwise unable to identify themselves and who are a danger to themselves or others.
5. For those who are deceased and not otherwise identified.

Authorized and trained LVMPD personnel may only perform a facial recognition search during the course of lawful duties, in accordance with LVMPD established authorized uses and when one of the following conditions exist:

1. Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The LVMPD will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
2. Consent: The individual consents to have his image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a facial recognition search is not authorized and the search must stop immediately.
3. Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his lawful duties.

PROGRAM MANAGEMENT

Tech Ops will be responsible for deploying, managing, and controlling access to the facial recognition program. Tech Ops Lieutenant, or designee, will ensure that access to facial recognition software is restricted to LVMPD personnel in assignments that require access to the facial recognition system or searches. Facial recognition will only be used for official and legitimate law enforcement purposes. Any misuse of facial recognition data may result in disciplinary action, up to termination.

The LVMPD is authorized to access and perform facial recognition searches utilizing the following external repositories:

1. Mugshots database.
2. Vigilant Solutions FaceSearch database.

Before access to the LVMPD facial recognition system is authorized, the LVMPD will require individuals to participate in training on the implementation of and adherence to this facial recognition policy.

PROCEDURE

All requests for facial recognition analysis will require a "probe photo." A probe photo is a still photograph depicting the face of the subject whose identity is unknown. For the most accurate results, this photo needs to be of the best quality possible and ideally an original, not a copy of a copy.

Requesting investigator will:

1. Submit a formal request via email to Tech Ops, which will include the following:
   a. Probe photograph of an unknown subject and descriptors provided by victim/witnesses (estimated age, height, weight, race, tattoos or other unique identifiers).
   b. Event number.
   c. Nature of the crime.
   d. Investigator's assignment.

Tech Ops FaceSearch Examiner will:

2. Analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a facial recognition search.
3. Initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
4. In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
5. The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner from Tech Ops. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
   a. If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
   b. If candidates are found, examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by another authorized, trained examiner.

FACIAL RECOGNITION RESULTS

All entities receiving the results of a facial recognition investigation must be cautioned that the resulting candidate images do not provide positive identification of any subject and are considered advisory in nature as an investigative lead only. Resulting candidate images do not establish probable cause to obtain an arrest warrant without further investigation and other facts or evidence. Any possible connection or involvement of the subject to the investigation must be determined through additional investigative methods. (8/18)■

Las Vegas Metropolitan Police Department
Purchasing and Contracts
400 S. Martin L. King Blvd. Bldg. B 4th floor
Las Vegas, NV 89106
Phone:(702) 828-5788 Fax:(702) 828-0146
Tax ID No. 88-6000028

Blanket Purchase Order 4300027524-503

Order Date	07/01/2017
Last change date	N/A
Payment Terms	Net 30 Days
Inco Terms	DESTINATION PREPAID & ALLOWED
Inco Terms(Part 2)	N/A
Validity Period	07/01/2017-06/30/2018
Reference Number	604526
Confirmation By	Scott Dye
Contact Person	REGINA MOLESKI
Phone Number	(702) 828-5504

Vendor Address
Vendor Number:517506
VIGILANT SOLUTIONS LLC
1152 STEALTH STREET
LIVERMORE CA 94551
Contact Person: Scott Dye
Phone/Fax: 503-339-5379 / 925-398-2113

Billing Address
LAS VEGAS METROPOLITAN POLICE DEPT
BUDGET / ACCOUNTING
400 S MARTIN L KING BLVD BLDG B 4th FLR
LAS VEGAS NV 89106 89106

Delivery Address
LAS VEGAS METROPOLITAN POLICE DEPT
NO DELIVERY REQUIRED.

In accordance with the Terms & Conditions of CBE 604526, approved 06/26/17
Agreement No.: 4660001092

Item	Material/Description	Quantity	UOM	Unit Price	Net Amount
10	INVESTIGATIVE DATA PLATFORM SUBSCRIPTION	1.00	EA	99,995.00 / EA	99,995.00
	ANNUAL SUBSCRIPTION FOR 1,501 TO 2000 USERS; JULY 6, 2017 THROUGH JULY 5, 2018.				
	CONTACT GINGER MOLESKI, SNCTC AA, WITH ANY QUESTIONS, 702-828-4022.				
	*** Item completely delivered ***				

Total $ 99,995.00

Las Vegas Metropolitan Police Department
Purchasing and Contracts
400 S. Martin L. King Blvd. Bldg. B 4th floor
Las Vegas, NV 89106
Phone:(702) 828-5788 Fax:(702) 828-0146
Tax ID No. 88-6000028

Blanket Purchase Order 4300027524-503

INSTRUCTIONS TO VENDOR:

This Purchase Order is subject to the Terms and Conditions incorporated herein by this reference. A complete copy of the Terms and Conditions is available on the Las Vegas Metropolitan Police Department's (LVMPD) website, http://www.lvmpd.com/purchasing/   LVMPD encourages the economic prosperity of all disadvantaged groups in the business community, and promotes full and open competition in all purchasing activities. If you have questions concerning how to prepare a bid, information that is available to you or you would like to discuss business opportunities within LVMPD, please contact us at telephone number (702) 828-5788.

Note: All Invoices must be submitted with the appropriate Purchase Order number referenced.

SIGNATURE   DATE: 07/01/2017

PHONE :

Las Vegas Metropolitan Police Department
Purchasing and Contracts
400 S. Martin L. King Blvd. Bldg. B 4th floor
Las Vegas, NV 89106
Phone:(702) 828-5788 Fax:(702) 828-0146
Tax ID No. 88-6000028

Blanket Purchase Order 4300028903-503

Order Date	07/01/2018
Last change date	N/A
Payment Terms	Net 30 Days
Inco Terms	NO DELIVERY REQUIRED
Inco Terms(Part 2)	N/A
Validity Period	07/06/2018-07/05/2019
Reference Number	604526
Confirmation By	Scott Dye
Contact Person	SARAH DI LUNA
Phone Number	(702) 828-3157

Vendor Address
Vendor Number:517506
VIGILANT SOLUTIONS LLC
1152 STEALTH STREET
LIVERMORE CA 94551
Contact Person: Scott Dye
Phone/Fax: 503-339-5379 / 925-398-2113

Billing Address
LAS VEGAS METROPOLITAN POLICE DEPT
BUDGET / ACCOUNTING
400 S MARTIN L KING BLVD BLDG B 4th FLR
LAS VEGAS NV 89106
LAS VEGAS METROPOLITAN POLICE DEPT

Delivery Address
LAS VEGAS METROPOLITAN POLICE DEPT
NO DELIVERY REQUIRED.

In accordance with the Terms & Conditions of CBE 604526, approved
Agreement No.: 4660001092

Item	Material/Description	Quantity	UOM	Unit Price	Net Amount
10	INVESTIGATIVE DATA PLATFORM SUBSCRIPTION	1.00	EA	101,990.00 / EA	101,990.00
	ANNUAL SUBSCRIPTION FOR 1,501 TO 2000 USERS JULY 6, 2018 THROUGH JULY 5, 2019				
	Quote #LMP-0654-01				
	In accordance with the Terms & Conditions of CBE 604526, approved 06/26/17.				
	CONTACT SNCTC AA, WITH ANY QUESTIONS, 702-828-4022.				
	*** Item completely delivered ***				

Total $ 101,990.00

Las Vegas Metropolitan Police Department
Purchasing and Contracts
400 S. Martin L. King Blvd. Bldg. B 4th floor
Las Vegas, NV 89106
Phone:(702) 828-5788 Fax:(702) 828-0146
Tax ID No. 88-6000028

Blanket Purchase Order 4300028903-503

INSTRUCTIONS TO VENDOR:

This Purchase Order is subject to the Terms and Conditions incorporated herein by this reference. A complete copy of the Terms and Conditions is available on the Las Vegas Metropolitan Police Department's (LVMPD) website, http://www.lvmpd.com/purchasing/ LVMPD encourages the economic prosperity of all disadvantaged groups in the business community, and promotes full and open competition in all purchasing activities. If you have questions concerning how to prepare a bid, information that is available to you or you would like to discuss business opportunities within LVMPD, please contact us at telephone number (702) 828-5788.

Note: All Invoices must be submitted with the appropriate Purchase Order number referenced.

SIGNATURE   DATE: 07/01/2018

PHONE :

160223

INVOICE

Vigilant Solutions, Inc.
1152 Stealth Street
Livermore CA 94551
United States
Ph: (925) 398-2079 Fax: (925) 398-2113

VIGILANT
S O L U T I O N S

Page Number	1 of 1
Request Date	06/29/2018
Sold To	600921
Ship To	600921
Branch Plant	10204
Customer PO	4300028903-503
Order Number	10891 S5
Invoice	17105 RI
Invoice Date	~~06/29/2018~~ 7/1/2018

Sold To:

Las Vegas Metro Police Department
400 S. Martin L King Blvd
Bldg B 4th Floor
Attn: Budget/Accounting
Las Vegas NV 89106
United States

Attn: Rich Hoggan
Ph: 702-828-1365

3119001372

Ship To:

FY19

Las Vegas Metro Police Department
400 S. Martin L King Blvd
Bldg B 4th Floor
Attn: Budget/Accounting
Las Vegas NV 89106
United States

Attn: Rich Hoggan
Ph: 702-828-1365

Project	Order By	Order Date	Ship Method	Carrier	Inco Terms
IDP Renewal for Las Vegas Metro PD	LMP	06/29/2018			

Line No	Item Number	Description	Ship Date	Ship/Back /Cancel	Unit Price	Extended Price	Tax
1.000	VS-IDP-06	INVESTIGATIVE DATA PLATFORM FOR 1,501 TO 2000 SWORN Period of Performance is July 2018 through June 2019.	06/29/2018	1 S	101990.00	101990.00	N

				Tax Rate 0 %		0 %
Terms		Net 30 Days		Sales Tax		
Net Due Date		7/29/2018		Total Order		101990.00

'18 JUL 18 AM11:44 ACCTG

5001705359
28029   7/17/18

	Vigilant Solutions LLC 2021 Las Positas Court - Suite # 101 Livermore, California 94551 (P) 503-339-5379 (F) 925-398-2113	**Be smart. Be safe.** **Be Vigilant.**
VIGILANT **SOLUTIONS**		

Attention:	Las Vegas Metro PD		Date	6/9/2017
Project Name:	IDP 2017		Quote Number:	SDY-0110-02

PROJECT QUOTATION

We at Vigilant Solutions are pleased to quote the following systems for the above referenced project:

Qty	Item #	Description

(1)	VS-IDP-06	**Investigative Data Platform - Annual Subscription for 1,501 to 2,000 members**
		
		• Commercial LPR Data access - For 1,501 to 2,000 members
		   o Access to all Vigilant commercially acquired national vehicle location data
		   o Unlimited use by authorized agency personnel to complete suite of LEARN data analytics
		   o Includes full use of hosted/managed LPR server account via LEARN
		• FaceSearch with Vigilant Image Gallery Access For 1,501 to 2,000 members
		   o Access to all agency/shared images and Vigilant Image Gallery
		   o Unlimited use by authorized agency personnel to all FaceSearch tools
		   o Image gallery of up to 200,000 images

Subtotal Price (Excluding sales tax)		**$99,995.00**

Quote Notes:

1. All prices are quoted in USD and will remain firm and in effect for 30 days.
2. All software to have standard one (1) year warranty for manufacturer defects.
3. Software is manufactured under strict Vigilant Solutions standard.
4. This Quote is provided per our conversation & details given by you – not in accordance to any written specification.
5. Annual IDP renewal 2nd yr. 2018 $101,990.00
6. Annual IDP renewal 3rd yr. 2019 $103,990.00
7. Annual IDP renewal 4th yr. 2020 $105,990.00
8. Annual IDP renewal 5th yr. 2021 $107,990.00

Quoted by: Scott Dye - 503-339-5379 - scott.dye@vigilantsolutions.com

Total Price (Excluding sales tax)	**$99,995.00**

VIGILANT SOLUTIONS – INVESTIGATIVE DATA PLATFORM
STATE AND LOCAL LAW ENFORCEMENT AGENCY AGREEMENT

This Agreement is made and entered into effective 6/13/2017 _____(the "Effective Date") between Vigilant Solutions, LLC, a Delaware company ("**Vigilant**") and Las Vegas Metropolitan Police Department, ("**Agency**").

A. Vigilant stores and disseminates to law enforcement agencies publicly and commercially gathered license plate recognition (LPR) data and booking images as a valued added component of the Vigilant law enforcement package of software; and

B. Agency desires to obtain access to Vigilant's Software Service (defined below) with available publicly and commercially collected LPR data via the Law Enforcement Archival Reporting Network (LEARN) server and publicly and commercially collected booking images via the FaceSearch server; and

C. Agency may separately purchase LPR hardware components from Vigilant and/or its authorized reseller for use with the Software Service (as defined below);

NOW, THEREFORE, in consideration of the mutual agreements contained herein and other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the parties, the parties agree as follows:

1. **Definitions.**
   (a) **Booking Images.** Refers to both LEA Booking Images and Commercial Booking Images.
   (b) **Commercial Booking Images.** Refers to images collected by commercial sources and available on the Software Service with a paid subscription.
   (c) **Commercial LPR Data.** Refers to LPR data collected by private commercial sources and available on the Software Service with a paid subscription. Vigilant represents and warrants to Agency that it has the right to grant the license to Agency in accordance with this Agreement.
   (d) **Confidential Information.** Refers to any and all of the following provided by Vigilant to Agency (i) rights of Vigilant associated with works of authorship, including exclusive exploitation rights, copyrights, moral rights and mask works, trademark and trade name rights and similar rights, trade secrets rights, patents, designs, algorithms and other industrial property rights, other intellectual and industrial property and proprietary rights of every kind and nature, whether arising by operation of law, by contract or license, or otherwise; and all registrations, applications, renewals, extensions, combinations, divisions or reissues of the foregoing; (ii) product specifications, data, know-how, formulae, compositions, processes, designs, sketches, photographs, graphs, drawings, samples, inventions and ideas, and past, current and planned research and development; (iii) current and planned manufacturing and distribution methods and processes, customer lists, current and anticipated customer requirements, price lists, market studies, and business plans; (iv) computer software and programs (including object code and source code), database technologies, systems, structures, architectures, processes, improvements, devices, discoveries, concepts, methods, and information of Vigilant; (v) any other information, however documented, of Vigilant that is a trade secret within the meaning of applicable state trade secret law or under other applicable law, including but not limited to the Software Service, the Commercial LPR Data and the Booking Images; (vi) information concerning the business and affairs of Vigilant (which includes historical financial statements, financial projections and budgets, historical and projected sales, capital spending budgets and plans, the names and backgrounds of key personnel, contractors, agents, suppliers and potential suppliers, personnel training techniques and materials, and purchasing methods and techniques, however documented; and (vii) notes, analysis, compilations, studies, summaries and other material prepared by or for Vigilant

containing or based, in whole or in part, upon any information included in the foregoing. Notwithstanding the foregoing, Confidential Information shall not include date or information that is: (a) generally publicly known, (b) learned from third persons with a legal right to disclose such information to Agency, or (c) independently created by Agency through efforts in no manner associated with or arising from any disclosure made by Vigilant.

(e) **LEA.** Refers to a law enforcement agency.

(f) **LEA Booking Images.** Refers to images collected by LEAs and available on the Software Service for use by other LEAs. LEA Booking Images are freely available to LEAs at no cost and are governed by the contributing LEA's policies.

(g) **LEA LPR Data.** Refers to LPR data collected by LEAs and available on the Software Service for use by other LEAs. LEA LPR Data is freely available to LEAs at no cost and is governed by the contributing LEA's retention policy.

(h) **LPR Data.** Refers to both LEA LPR Data and Commercial LPR Data.

(i) **License Plate Recognition ("LPR").** Refers to the process of utilizing cameras, either stationary or mounted on moving vehicles, to capture and interpret images of vehicle license plates.

(j) **Software Service.** Refers to a web based (hosted) suite of software applications consisting of analytical and investigative software located on a physical database server that also hosts LPR Data or Booking Images.

(k) **User.** Refers to an individual who is an agent and/or officer of Agency and who is authorized by Agency to access the Software Service on behalf of Agency through login credentials provided by Agency.

2. **Licensed Access to the Software Service.**

(a) **Grant of License.** During the term of this Agreement, Vigilant grants Agency a non-exclusive, non-transferable right and license to access the Software Service for use in accordance with the terms of this Agreement.

(b) **Authorized Use.** Agency is prohibited from accessing the Software Service other than for law enforcement purposes.

(c) **Ownership of Commercial LPR Data, Commercial Booking Images, FaceSearch Software and LEARN Software.** Except for the rights expressly granted by Vigilant to Agency under this Agreement, Vigilant retains all title and rights to the Commercial LPR Data, Commercial Booking Images, FaceSearch Software and the LEARN Software. Nothing contained in this Agreement shall be deemed to convey to Agency or to any other party any ownership interest in or to any LPR Data, Booking Images, FaceSearch Software or LEARN Software.

(d) **Restrictions on Use of Software Service.** Except as expressly permitted under this Agreement, Agency agrees that it shall not, nor will it permit a User or any other party to, without the prior written consent of Vigilant, (i) copy, duplicate or grant permission to the Software Service or any part thereof; (ii) create, attempt to create, or grant permission to the source program and/or object program associated with the Software Service; (iii) decompile, disassemble or reverse engineer any software component of the Software Service for any reason, including, without limitation, to develop functionally similar computer software or services; or (iv) modify, alter or delete any of the copyright notices embedded in or affixed to the copies of any components of the Software Service.

(e) **Third Party Software and Data.** If and to the extent that Vigilant incorporates the software and/or data of any third party into the Software Service, including but not limited to the LEA LPR Data, and use of such third party software and/or data is not subject to the terms of a license agreement directly between Agency and the third party licensor, the license of Agency to such third party software and/or data shall be defined and limited by the license granted to Vigilant by such third party and the license to the Software Service granted by Vigilant under this Agreement. Agency specifically acknowledges that the licensors of such third party software and/or data shall retain all ownership rights thereto, and Agency agrees that it shall not (i) decompile, disassemble or reverse engineer such third party software or otherwise use such third party software for any reason except as expressly permitted herein; (ii) reproduce the data therein for purposes other than those specifically permitted under this Agreement; or (iii) modify, alter or delete any of

VIGILANT

the copyright notices embedded in or affixed to such third party software.

(f)   **Non-Exclusive Licensed Access.** Agency acknowledges that the right or ability of Vigilant to license other third parties to use the Software Service is not restricted in any manner by this Agreement, and that it is Vigilant's intention to license a number of other LEAs to use the Software Service. Vigilant shall have no liability to Agency for any such action.

3.   **Other Matters Relating to Access to Software Service.**

(a)   **Accessibility.** The Software Service, LPR Data, Booking Images and associated analytical tools are accessible to LEAs ONLY and are accessible pursuant to one of the following two methods:

(1)   **Application Programming Interface (API).** The API access method allows for integration of the LPR Data and Booking Images into external third-party analytic tools. The API does NOT provide ownership rights to the LPR Data or Booking Images, only access during the subscription period. The API is available only in conjunction with a Software Service Subscription for an additional fee.

(b)   **Access to LEA LPR Data.** LEA LPR Data is provided as a service to LEAs at no additional charge.

(c)   **Access to LEA Booking Images.** LEA Booking Images are provided as a service to LEAs at no additional charge.

(d)   **Eligibility.** Agency shall only authorize individuals who satisfy the eligibility requirements of "Users" to access the Software Service. Vigilant in its sole discretion may deny Software Service access to any individual based on such person's failure to satisfy such eligibility requirements.

(e)   **Account Security (Agency Responsibility).**

(1)   Agency shall be responsible for assigning an account administrator who in turn will be responsible for assigning to each of Agency's Users a username and password (one per user account). Agency will purchase a set of user licenses. Agency will cause the Users to maintain username and password credentials confidential and will prevent use of such username and password credentials by any unauthorized person(s). Agency shall notify Vigilant immediately if Agency believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Agency must notify Vigilant immediately if Agency becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

(2)   User logins are restricted to agents and officers of the Agency. No User logins may be provided to agents or officers of other local, state, or Federal LEAs. LPR Data must reside within the Software Service and cannot be copied to another system, unless Agency purchases Vigilant's API. Booking Images must reside within the Software Service and cannot be copied to another system, unless Agency purchase Vigilant's API.

(f)   **Data Sharing.** If Agency is a generator as well as a consumer of LEA LPR Data or LEA Booking Images, Agency at its option may share its LEA LPR Data and/or LEA Booking Images with similarly situated LEAs who contract with Vigilant to access the Software Service (for example, LEAs who share LEA LPR Data with other LEAs).

(g)   **Subscriptions.** Software Service software applications, LPR Data and Booking Images are available to Agency and its Users on an annual subscription basis based the size of the agency.

(h)   **Available API.** Vigilant offers an API whereby Agency may load LPR Data and/or Booking Images and provide for ongoing updating of LPR Data or Booking Images into a third-party system of Agency's choosing (the "API"). This service is offered as an optional service and in addition to the annual subscription fee described in Section 3(g). Vigilant will not charge a fee for API for Agency's Booking Images.

VIGILANT
SOLUTIONS

4.   Restrictions on Access to Software Service.

(a)   **Non Disclosure of Confidential Information.** Agency and each User will become privy to Confidential Information during the term of this Agreement. Agency acknowledges that a large part of Vigilant's competitive advantage comes from the collection and analysis of this Confidential Information and Agency's use, except as expressly permitted under this Agreement, and disclosure of any such Confidential Information would cause irreparable damage to Vigilant.

(b)   **Restrictions.** As a result of the sensitive nature of the Confidential Information, Agency agrees, except to the extent expressly permitted under this Agreement, (i) not to use or disclose, directly or indirectly, and not to permit Users to use or disclose, directly or indirectly, any LPR location information obtained through Agency's access to the Software Service or any other Confidential Information; (ii) not to download, copy or reproduce any portion of the LPR Data and/or Booking Images and other Confidential Information; and (iii) not to sell, transfer, license for use or otherwise exploit the LPR Data and or Booking Images and other Confidential Information in any way. Additionally, Agency agrees to take all necessary precautions to protect the Confidential Information against its unauthorized use or disclosure and exercise at least the same degree of care in safeguarding the Confidential Information as Agency would with Agency's own confidential information and to promptly advise Vigilant in writing upon learning of any unauthorized use or disclosure of the Confidential Information.

(c)   **Third Party Information.** Agency recognizes that Vigilant has received, and in the future will continue to receive, from LEAs associated with Vigilant their confidential or proprietary information ("**Associated Third Party Confidential Information**"). By way of example, Associated Third Party Confidential Information includes LEA LPR Data and/or LEA Booking Images. Agency agrees, except to the extent expressly permitted by this Agreement, (i) not to use or to disclose to any person, firm, or corporation any Associated Third Party Confidential Information, (ii) not to download, copy, or reproduce any Associated Third Party Confidential Information, and (iii) not to sell, transfer, license for use or otherwise exploit any Associated Third Party Confidential Information. Additionally, Agency agrees to take all necessary precautions to protect the Associated Third Party Confidential Information against its unauthorized use or disclosure and exercise at least the same degree of care in safeguarding the Associated Third Party Confidential Information as Agency would with Agency's own confidential information and to promptly advise Vigilant in writing upon learning of any unauthorized use or disclosure of the Associated Third Party Confidential Information. Notwithstanding the foregoing, Third Party Confidential Information shall not include data or information that is: (a) generally publicly known, (b) learned from third persons with a legal right to disclose such information to Agency, or (c) independently created by Agency through efforts in no manner associated with or arising from any disclosure made by Vigilant or any third party. In addition, Agency shall not be bound by this provision until it has been informed or has reason to know that Vigilant has received confidential or proprietary information from LEA's. If Agency or any User is requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoena, civil investigative demand or other similar process) to disclose any of the Third Party Confidential Information, Agency shall provide Vigilant with prompt written notice of such requirement so that Vigilant may seek a protective order or other appropriate remedy and/or waive compliance with the provision of this agreement, but disclosure by Agency or any User after delivering such notice shall not be deemed a default under this Agreement.

(d)   **Non-Publication.** Agency shall not create, publish, distribute, or permit any written, electronically transmitted or other form of publicity material that makes reference to the Software Service or this Agreement without first submitting the material to Vigilant and receiving written consent from Vigilant thereto. This restriction is specifically intended to ensure consistency with other media messaging. The foregoing shall not prevent internal Agency communication regarding the LEARN Software Service or this Agreement, or communication with Agency's attorneys and advisors, and Vigilant acknowledges that the entering into this Agreement shall be of public record by virtue of Agency's reporting requirements for contracts awarded by Agency.

VIGILANT
SOLUTION

(e)   **Non-Disparagement.** Agency agrees not to use proprietary materials or information in any manner that is disparaging. This prohibition is specifically intended to preclude Agency from cooperating or otherwise agreeing to allow photographs or screenshots to be taken by any member of the media without the express consent of Vigilant. Agency also agrees not to voluntarily provide ANY information, including interviews, related to Vigilant, its products or its services to any member of the media without the express written consent of Vigilant.

(f)   **Survival of Restrictions and Other Related Matters.**

(1)   Agency agrees to notify Vigilant immediately upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this **Section 4** by Agency or any User, and Agency shall reasonably cooperate with Vigilant to regain possession of the Confidential Information, prevent its further unauthorized use, and otherwise prevent any further breaches of this **Section 4**.

(2)   Agency agrees that a breach or threatened breach by Agency or a User of any covenant contained in this **Section 4** will cause irreparable damage to Vigilant and that Vigilant could not be made whole by monetary damages. Therefore, Vigilant shall have, in addition to any remedies available at law, the right to seek equitable relief to enforce this Agreement.

(3)   No failure or delay by Vigilant in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise of any such right, power or privilege preclude any other or further exercise thereof.

(4)   The restrictions set forth in this **Section 4** shall survive the termination of this Agreement for a period of two (2) years.   ·

5.   **Fees, Term and Termination.**

(a)   **Fees.** Initial Service Fee for the Investigative Data Platform for Annual Subscription for 1,501 to 2,000 officers and agents of Agency is $99,995, for the period of July 6, 2017 through July 5, 2018. If the Agency chooses to renew this agreement, pricing for the Investigative Data Platform fees for Year 2 shall be $101,990; Year 3 shall be $103,990; Year 4 shall be $105,990 and Year 5 shall be $107,990.

(b)   **Term.** The Initial Term of this Agreement shall be for a term of one (1) year effective July 6, 2017 through July 5, 2018. (the "Initial Term").

(c)   **Agreement Renewals.** The Agency has the option to renew this Agreement for an additional four (4) one-year periods from its expiration date.

(d)   **Agreement Extension.** Agency reserves the option to temporarily extend this Agreement for periods up to ninety (90) calendar days from its expiration date for any reason.

(e)   **Renewal Invoicing.** Sixty (60) days prior to the expiration of the Initial Term and each subsequent Service Period, Vigilant will provide Agency with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a "Service Period"). This Agreement will be extended for a Service Period upon Agency's payment of that Service Period's Service Fee, which is due 30 days prior to the expiration of the Initial Term or the existing Service Period, as the case may be. Agency may also pay in advance for more than one Service Period.

(f)   **Termination.**

(1)   Agency may terminate this Agreement upon thirty (30) days prior written notice to Vigilant for any reason. Agency shall not be entitled to a refund of the annual subscription fee, or any portion thereof, if Agency terminates the agreement prior to the end of a Service Period without cause. If Agency termination notice is based on an alleged breach by Vigilant, then Vigilant shall have thirty (30) days from the date of its receipt of Agency's notice of termination, which shall set forth in detail Vigilant's purported breach of this agreement, to cure the alleged breach. If Agency terminates this agreement prior to the end of a Service Period for breach of a material term or condition of this Agreement, Vigilant shall refund to Agency an amount calculated by multiplying the total amount of Service Fees for the Software Service paid by Agency for the then- current Service Period by the percentage resulting from dividing the number

of days remaining in the then-current Service Period, by 365.

(2)   Vigilant may terminate this Agreement by providing thirty (30) days written notice to Agency for any reason. If Vigilant's termination notice is based on an alleged breach by Agency, then Agency shall have thirty (30) days from the date of its receipt of Vigilant's notice of termination, which shall set forth in detail Agency's purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Vigilant Agency has not reasonably cured the described breach of this Agreement, Agency shall immediately discontinue all use of the LEARN Software Service. If Vigilant terminates this Agreement prior to the end of a Service Period for breach, no refund for any unused Service Fees will be provided. If Vigilant terminates this Agreement prior to the end of a Service Period for no reason, and not based on Agency's failure to cure the breach of a material term or condition of this Agreement, Vigilant shall refund to Agency an amount calculated by multiplying the total amount of Service Fees paid by Agency for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365.

(g)   **Effect of Termination.** Upon termination or expiration of this Agreement for any reason, all licensed rights granted in this Agreement will immediately cease to exist and Agency must promptly discontinue all use of the Software Service, erase all LPR Data and/or Booking Images accessed through the Software Service from its computers, including LPR Data and/or Booking Images transferred through an API, and return all copies of any related documentation and other materials.

6.   **Miscellaneous.**

(a)   **Training.** Webinar training is ongoing and no cost to Agency. On-property training will be provided by Vigilant at no cost to Agency.

(b)   **Notices.** Any notice under this Agreement must be written. Notices must be addressed to the recipient and either (i) hand delivered; (ii) placed in the United States mail, certified, return receipt requested; (iii) deposited with an overnight delivery service; or (iv) sent via e-mail and followed with a copy sent by overnight delivery or regular mail, to the address or e-mail address specified below. All other notices are effective upon receipt. A failure of the United States Postal Service to return the certified mail receipt to the dispatcher of such notice will not affect the otherwise valid posting of notice hereunder.

Addresses for all purposes under this Agreement are:

Vigilant Solutions, LLC	Agency: Las Vegas Metropolitan Police Department
Attn: Steve Cintron	Attn: Richard Hoggan, CFO
2021 Las Positas Court, Suite #101	Address: 400B S Martin L King Blvd.
Livermore, California 94551	Las Vegas, NV 89106
Telephone: 925-398-2079	Telephone: 702- 828-1365
E-mail: steve.cintron@vigilantsolutions.com	E-mail: r7762h@lvmpd.com
with a copy to:	
Holland, Johns & Penny, L.L.P.	Las Vegas Metropolitan Police Department
Attn: Margaret E. Holland	Attn: Purchasing Unit
306 West Seventh Street, Suite 500	400 B S Martin L King Blvd.
Fort Worth, Texas 76102	Las Vegas, NV 89106
Telephone: 817-335-1050	Telephone: 702-828-5788
E-mail: meh@hjpllp.com	puchasing@lvmpd.com

VIGILANT
SOLUTIONS

Either party may designate another address for this Agreement by giving the other party at least five (5) business days' advance notice of its address change. A party's attorney may send notices on behalf of that party, but a notice is not effective against a party if sent only to that party's attorney.

(c)   **Disclaimer.** Vigilant makes no express or implied representations or warranties regarding Vigilant's equipment, website, online utilities or their performance, availability, functionality, other than a warranty of merchantability and fitness for the particular purpose of searching for license plate locations in the database and performing other related analytical functions. Any other implied warranties of merchantability or fitness for a particular purpose are expressly disclaimed and excluded.

(d)   **Limitations of Liability.** VIGILANT WILL NOT BE LIABLE FOR AGENCY'S USE OF THE LPR DATA, BOOKING IMAGES OR SOFTWARE SERVICE APPLICATIONS AND WILL NOT BE LIABLE TO AGENCY UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST OF BUSINESS). TO THE EXTENT THE FOREGOING LIMITATION OF LIABILITY IS PROHIBITED OR OTHERWISE UNENFORCEABLE VILIGANT'S CUMULATIVE LIABILITY TO AGENCY ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AGGREGATE OF ALL PAYMENTS MADE BY AGENCY UNDER THIS AGREEEMENT.

(e)   **Independent Contractor Status.** Each party will at all times be deemed to be an independent contractor with respect to the subject matter of this Agreement and nothing contained in this Agreement will be deemed or construed in any manner as creating any partnership, joint venture, joint enterprise, single business enterprise, employment, agency, fiduciary or other similar relationship.

(f)   **Assignment of this Agreement.** N e i t h e r p a r t y may not assign its rights or obligations under this Agreement to any party, without the express written consent of the other party.

(g)   **No Exclusivity.** Vigilant may at any time, directly or indirectly, engage in similar arrangements with other parties, including parties which may conduct operations in geographic areas in which Agency operates. Additionally, Vigilant reserves the right to provide LPR Data and Booking Images to third-party entities for purposes of promotions, marketing, business development or any other commercially reasonable reason that Vigilant deems necessary and appropriate. Vigilant shall not have the right to market the account that this Agency has, without the prior written approval.

(h)   **No Reliance.** Agency represents that it has independently evaluated this Agreement and is not relying on any representation, guarantee, or statement from Vigilant or any other party, other than as expressly set forth in this Agreement.

(i)   **Governing Law; Venue.** THIS AGREEMENT IS GOVERNED BY AND INTERPRETED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEVADA WITHOUT REGARD TO CONFLICTS-OF-LAWS PRINCIPLES. THE PARTIES HERETO CONSENT THAT VENUE OF ANY ACTION BROUGHT UNDER THIS AGREEMENT WILL BE IN CLARK COUNTY, NEVADA.

(j)   **Amendments.** Except as otherwise permitted by this Agreement, no amendment to this Agreement or waiver of any right or obligation created by this Agreement will be effective unless it is in writing and signed by both parties. Vigilant's waiver of any breach or default will not constitute a waiver of any other or subsequent breach or default.

(k)   **Entirety.** This Agreement and the Agency's purchase order, setting forth Vigilant's Software Service being purchased by Agency pursuant to this Agreement and the related product code and subscription price, represent the entire agreement between the parties. Except to the limited extent expressly provided in this **Section 6(j)**, no contrary or additional terms contained in any purchase order or other communication from Agency will be a part of this Agreement.

(l)   **Force Majeure.** Neither party will be liable for failure to perform or delay in performing any obligation under this Agreement if nonperformance is caused by an occurrence beyond the reasonable control of such party and without its fault or negligence such as acts of God or the public enemy, acts of the Government in either its

sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, delays of common carriers, or any other cause beyond the reasonable control of such party.

(m) **Severability.** If any provision of this Agreement is held to be invalid, illegal or unenforceable for any reason, such invalidity, illegality or unenforceability will not affect any other provisions of this Agreement, and this Agreement will be construed as if such invalid, illegal or unenforceable provision had never been contained herein.

(n) **Price Adjustments.** Vigilant has the right to increase or decrease the annual Service Fee from one Service Period to another; *provided, however,* that in no event will a Service Fee be increased by more than the greater of (i) 2% of the prior Service Period's Service Fees. If Vigilant intends to adjust the Service Fee for a subsequent Service Period, it must give Agency notice of the proposed increase on or before the date that Vigilant invoices Agency for the upcoming Service Period. Any price decreases should be provided to Agency.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by persons duly authorized as of the date and year first above written.

Company:	Vigilant Solutions, LLC
Authorized Agent:	Bill Quinlan
Title:	Vice President Sales Operations
Date:	6/12/2017
Signature:	*Bill Quinlan* (DocuSigned by: C03F1A0E3D6E47C...)
Agency:	Las Vegas Metropolitan Police Department
Authorized Agent:	Richard Hoggan
Title:	CFO
Date:	*Rich Hoggan* (DocuSigned by: 9B2583BF6A77415...)
Signature:	6/13/2017

APPROVED AS TO FORM:

SANTORO, WHITMIRE, LTD

andy Glendon (DocuSigned by:)   6/13/2017

Andrew J. Glendon, Esq.   Date
Legal Counsel

.

INVOICE

Vigilant Solutions, Inc.
2021 Las Positas Court Suite #101
Livermore, CA 94551
Ph: (925) 398-2079 Fax: (925) 398-2113

_160223_

Page Number	1 of 1
Request Date	07/03/2017
Sold To	600921
Ship To	600921
Branch Plant	10204
Customer PO	4300027524-503
Order Number	6644 S5
Invoice	10880 RI
Invoice Date	07/05/2017

Sold To:

Las Vegas Metro Police Department
400 S Martin L King Blvd
Bldg B 4th Floor
Las Vegas NV 89106
United States

Attn: Rich Hoggan
Ph: 702-828-1365

Ship To:

Las Vegas Metro Police Department
400 S Martin L King Blvd
Bldg B 4th Floor
Las Vegas NV 89106
United States

Attn: Rich Hoggan
Ph: 702-828-1365

Project	Order By	Order Date	Ship Method	Carrier	Inco Terms
	SDY	07/03/2017	.		.

Line No	Item Number	Description	Ship Date	Ship/Back /Cancel	Unit Price	Extended Price	Tax
1.000	VS-IDP-06	INVESTIGATIVE DATA PLATFORM FOR 1,501 TO 2000 SWORN	07/05/2017	1 S	99995.00	99995.00	N

			Tax Rate 0 %	0 %
Terms	Net 30 Days		Sales Tax	
Net Due Date	8/4/2017		Total Order	99995.00

'17 JUL 18 AM11:31 ACCTG

_3118001216_

'17 JUL 12 PM3:04
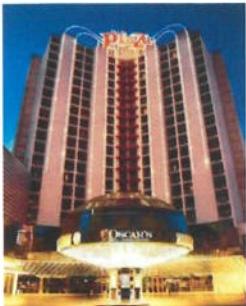
NLPOA Southern Nevada Chapter Law Enforcement Training
Friday, January 18, 2019

Plaza Hotel, 1 Main Street, Convention Hall 3rd floor
Las Vegas, Nevada 89101

7:00 a.m. - 8:00 a.m. – Registration

8:00 a.m. - 9:30 a.m.
Hybrid Gangs in the Clark County School District
Officer Steven Ufford, CCSD Police Department, NV

An overview and current trends of hybrid gangs in the Clark County School District, Nevada (5th largest school district, w/325,531 students).

9:30 a.m. - 11:30 a.m.
Investigations – FBI Next Generation Identification
Greg Scarbro, Unit Chief
FBI Criminal Justice Information Services Division
Biometric Services Section, W. Virginia

Overview of the NGI ten print, latent print, facial recognition, cold case/unknown deceased and criminal history system utilized by the Nation's Law Enforcement community

11:30 a.m. - 1:00 p.m. Luncheon
Speaker Cedric Crear, Ward 5 Councilman

1:00 p.m. - 5:00 p.m.
Patron Saints of the Mexican Drug Underworld and Cartels
Robert Almonte, former U.S. Marshal & former El Paso Police Department. Texas

Investigations, current updates, and an overview of the Mexican Drug Underworld and Cartels.
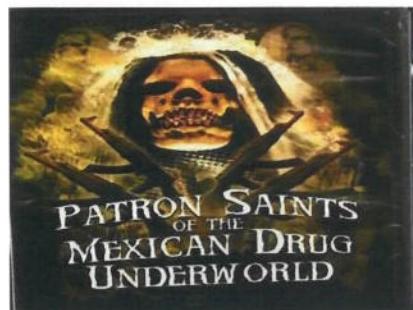
Law Enforcement Only – FREE to NLPOA Southern NV members
$65 Fee Registration includes lunch & training certificate
Register online at www.nlpoasouthernnv.com or www.nlpoa.com
More Information: Antonio Rodriguez- Antonio Rodriguez so.nv.nlpoa@gmail.com
Rafael Gil nlpoa905@gmail.com

The hotel is situated in Downtown Las Vegas 1-800-634-6575.
Parking is $20 or park in the city of Las Vegas garage 500 S. Main Street
Registration Deadline – January 14, 2019

Las Vegas Metropolitan Police Department
Request for Cold Case Probe Images

Priority: LVMPD Everyone Notices | Normal Priority

Title: Request for Cold Case Probe Images

Body: The Technical Operations Section (Tech Ops) is responsible for the management and use of the facial recognition program. Our specially trained personnel in Fusion Watch are the ones that deploy the technology on a 24/7 basis. Since the initial launch, the unit has been quite successful in generating leads to help investigators solve numerous crimes that would have likely gone unsolved.

On May 8th, 2019, this unit will be conducted an internal workshop designed to enhance their skills and experience in using the facial recognition technology. This workshop will also serve the dual purpose of resolving any and all cold cases. As such, if you are a detective that has a cold case(s) with a picture of a suspect that you always wished you could solve, we may be able to help. All you need to do is send the probe images to fusionwatch@lvmpd.com with the attached request form and allow us to help resolve some of these cold cases. Please ensure that the pictures are clear and follow our submission policy 5/206.19.

Additionally, if you are interested in learning more about the Tech Ops facial recognition program, we recommend you take the UMLV course titled "Face Recognition Requests." The training video is only 4.5 minutes long and it provides good information on the process for submitting a facial recognition request.

Any questions may be directed to Tech Ops Program Manager Detective K. Bluth at

Expires: 5/16/2019 12:00 AM

Created at 5/2/2019 7:51 AM by Michelle Alley
Last modified at 5/2/2019 8:42 AM by Michelle Alley

Las Vegas Metropolitan Police Department

Technical Operations Section

Facial Recognition Assistance Request

○ Emergency request

(may require supervisor approval and

Fusion Watch call-out)

○ Regular request

(turnaround time up to 72 hours)

Have you completed the mandatory

Face Search training?   ○ Yes   ○ No

Requestor name and P#:

Requesting bureau and section:

Event number:

Crime being investigated:

Circumstances of crime (brief synopsis):

Is there a named person of interest?   ○ Yes   ⦿ No

If so, provide as much information as possible regarding the person of interest:

Was there a witness?   ○ Yes   ○ No

If so, please detail the suspect description provided by the witness:

Signature of requestor: _____

Please print, sign, and email this signed form, along with the highest quality still photo possible, to FusionWatch@LVMPD.com. By submitting this form, the requestor acknowledges that criminal predicate exists for the person in the photo provided and that any requests for assistance with facial recognition for anyone pictured who is not a suspect in a crime could result in major discipline under LVMPD policy, 5/105.21—Accessing/Disseminating Information. CURIOSITY CHECKS ARE NOT ALLOWED.

Las Vegas Metropolitan Police Department

Technical Operations Section

Facial Recognition Assistance Request

○ Emergency request
(may require supervisor approval and
Fusion Watch call-out)

○ Regular request
(turnaround time up to 72 hours)

Requestor name and P#:

Requesting bureau and section:

Event number:

Crime being investigated:

Suspect/Victim/Witness:

Suspect age range:

Suspect race:

Possible name/moniker:

Suspect social media URLs:

Describe the circumstances of the crime:

Electronic signature of requestor:

Please electronically sign and email this form, along with the highest quality still photo possible, to FusionWatch@LVMPD.com. By submitting this form, the requestor acknowledges that criminal predicate exists for the person in the photo provided, or that the person in the photo is a victim or witness related to a criminal investigation, and that any requests for assistance with facial recognition for anyone pictured who is not associated with a criminal investigation could result in major discipline under LVMPD policy, 5/105.21—Accessing/Disseminating Information. CURIOSITY CHECKS ARE NOT ALLOWED.

Las Vegas Metropolitan Police Department
Tech Ops Section – Facial Recognition Program

Priority: LVMPD Everyone Notices | Normal Priority
Title: Tech Ops Section – Facial Recognition Program
Body: **Language:**

The Technical Operations Section is excited to announce an initial 90 day deployment of our Facial Recognition program. This technology is often referred to as "FaceSearch" and it offers tremendous potential in identifying persons of interest that are unknown at the time of investigation. These initial 90 days will serve as a beta test so we can continue to fine tune the process and procedures related to this new program. We are also limiting the use of the program to Homicide, Sexual Assault, Robbery, Theft Crimes, and VICE for this initial launch. Once we identify and resolve potential challenges, we will finalize the program and launch agency-wide. In the meantime, below is a brief synopsis of what the program is, how it will function, and why it is expected to have an impact on violent crime.

WHAT

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The LVMPD has established the capability to conduct facial recognition searches in support of law enforcement activities. This capability is primarily available through the facial recognition program, which is managed by the Tech Ops Section

HOW

Fusion Watch, which is a 24/7 component of the Tech Ops Section, will execute FaceSearch requests as outlined in the new facial recognition policy. The personnel in this unit have received extensive training in applying facial recognition technologies from the vendor, as well as from the FBI Facial Recognition Unit. This centralized approach combined with oversight from the FaceSearch Program Management Team, ensures the proper use of this new technology.

Investigators, who have completed the necessary awareness training for this program may submit a facial recognition request by contacting Fusion Watch via email or phone 24/7. This awareness training, which involves understanding the legal parameters and process for submitting a request, is required and it ensures more accurate results. Once the request is received and processed, the face search identification with the greatest probability will be provided to the investigator for further evaluation. Although this investigative lead may prove instrumental in identifying a suspect, it is not considered a positive identification or

probable cause without further investigation and additional evidence.

WHY

Although we are in the early stages of establishing this new technology, the potential this program offers is tremendous. With diligence and caution, we anticipate being able to help units identify a robbery suspect before a series unfolds, confirm the identity of a homicide victim without delay, and determine who the suspect is for just about any crime that was sufficiently captured on video. This technology, and the initial launch in particular, will likely come with some errors and several learning opportunities, but ultimately, we are confident it will prove to be quite useful for many investigations. More importantly, we hope the use of this technology in combination with some of our other technologies and programs (i.e. Cameras, ALPR, GRID Pattern Identifications, ShotSpotter, etc.) will result in a significant impact on violent crime within Southern Nevada.

Any questions may be directed to the Facial Recognition Program Managers, Detective Kelly Bluth or Sergeant Travis Cunningham.

LVMPD Technical Operations Section

Expires: 8/24/2018 12:00 AM

Created at 8/10/2018 2:01 PM by Michelle Grimes
Last modified at 8/10/2018 2:01 PM by Michelle Grimes

Las Vegas Metropolitan Police Department
Facial Recognition Program

Priority: LVMPD Everyone Notices | Normal Priority
Title: Facial Recognition Program
Body: **Tech Ops Section – Facial Recognition Program**

The Technical Operations Section is excited to announce we are about half way through our initial 90 day deployment of our Facial Recognition program. This technology is often referred to as "FaceSearch" and it offers tremendous potential in identifying persons of interest that are unknown at the time of investigation. The beta test period was limited to only five specific units including Homicide, Sexual Assault, Robbery, Theft Crimes, and VICE. The program was launched to limited units as we anticipated the launch would likely come with some errors and learning opportunities. Once we identify and resolve these potential challenges, we will finalize the program and launch agency-wide. In the meantime, below is a brief synopsis of the impressive impact the program has provided since the initial launch.

EARLY FINDINGS

Since launching, August 1, 2018, the investigative team has processed more than 50 requests. Of the requests that met the minimum requirements, the team has been able to identify a likely candidate in more than 60% of the cases. It is important to note that the majority of these are cases that would have otherwise likely gone unsolved. It is also important to advise the significance of some of these solved cases. A few involved criminal activity that had been occurring for some time and would have likely continued to occur without the successful identification through FaceSearch and the subsequent law enforcement interdiction. Some of the investigations the facial recognition team have assisted with include homicide, robbery, sex trafficking, burglary, grand larceny, battery, illegal firearms trafficking and more.

SYNOPSIS

Although we are in the early stages of establishing this new technology, the potential this program offers is tremendous. With diligence and caution, we anticipate being able to help units identify a robbery suspect before a series unfolds, confirm the identity of a homicide victim without

delay, and determine who the suspect is for just about any crime that was sufficiently captured on video.

HOW TO PARTICIPATE

Investigators, who have completed the necessary awareness training for this program and who are assigned to one of the predesignated units for the test phase, may submit a facial recognition request by contacting Fusion Watch via email or phone 24/7. Fusion Watch, which is a 24/7 component of the Tech Ops Section, will execute FaceSearch requests as outlined in the new facial recognition policy. The personnel in this unit have received extensive training in applying facial recognition technologies from the vendor, as well as from the FBI Facial Recognition Unit. This centralized approach combined with oversight from the FaceSearch Program Management Team, ensures the proper use of this new technology.

Any questions may be directed to the Facial Recognition Program Managers, Detective Kelly Bluth or Sergeant Travis Cunningham.

Expires:

LVMPD Technical Operations Section
10/26/2018 12:00 AM

Created at 10/12/2018 8:07 AM by Michelle Alley
Last modified at 10/12/2018 8:07 AM by Michelle Alley

Las Vegas Metropolitan Police Department

Update: Tech Ops Facial Recognition Program

Priority: LVMPD Everyone Notices | Normal Priority
Title: Update: Tech Ops Facial Recognition Program
Body: **Update: Tech Ops Facial Recognition Program**

The Technical Operations (Tech Ops) Section has completed the initial launch of the facial recognition program and the use of this resource is now being extended to all LVMPD personnel. This technology is often referred to as "FaceSearch" and it offers tremendous potential in identifying persons of interest that are unknown at the time of investigation.

Early Findings

Since launching, August 1, 2018, our Fusion Watch personnel have processed more than 207 face search requests. More importantly, our rate of success in identifying a likely candidate for the requests that involved a suitable photo has now reached 83%. It is also worth noting that many of these cases involved violent felony crimes.

Next Steps

The expanded use of this resource for all department members is very promising. We anticipate being able to help units identify a robbery suspect before a series unfolds, confirm the identity of a homicide victim without delay, and determine who the suspect is for just about any crime that was sufficiently captured on video.

How to Participate

Department policy requires any person submitting a facial recognition request to have received the correlated training. This training course is available through the UMLV portal via a short training video. This training is mandatory for police officers of the rank of Lieutenant and

below. The training course is found in the "My Online Courses" tab. The title of the training is "Face Recognition Requests". The training video is only approximately 4.5 minutes long, provides good information and instructs the student on the process of submitting a facial recognition request.

Any questions may be directed to the Facial Recognition Program Managers, Detective Kelly Bluth or Sgt. Travis Cunningham.

Expires: 2/20/2019 12:00 AM

Created at 2/6/2019 12:48 PM by Michelle Alley
Last modified at 2/6/2019 12:48 PM by Michelle Alley

Good Afternoon:

My company FaceFirst is a leading provider of facial recognition technology to law enforcement. We serve nearly 80 agencies.

I have been calling LVMPD to see if we can demonstrate this technology and was told to start with purchasing. Below are a coupl eof recent testimonials we received from clients.

FaceFirst is the leading provider of facial recognition technology to law enforcement and we recently received testimonials from our clients, here are 2 for your review.

1: I just wanted to send a positive note on two events regarding the new Face First program. Three tablets were upgraded with the test program last week. The very next day we used it on our first call. The residence we were in was a known flop house with several occupants. One male ran out the back into the garage to hide but was located and detained. The male was photographed and entered into the TACIDS system. A 99.97% match was provided on the male. A records check of the name and DOB provided the male had an active felony warrant and was a parolee at large.

2: Just wanted to drop you a note on how the facial recognition worked yesterday. Right after our weekly investigations' meeting I was assisting other detectives on a follow up of a kidnapping / robbery. We ended up at the suspect's house and contacted numerous people. I contacted two people who were not involved but were in the suspect's apartment. One had ID and had a PAL warrant and was immediately arrested. The other person, a female, had no ID and gave the name of a real person in AZ. It was obvious this female had been arrested before but the record's check showed no hits of a criminal record. At this point in the investigation she was not a suspect in the kidnapping and we did not have anything else on her we knew she was lying about her identity and were running out of detention time. I sent you the photo of her and within a couple of minutes we had her identified and learned she was a parolee at large. She was arrested for the warrant and identity theft...very helpful tool.

We would like to offer you a 45 minute WebEx demonstration and show you the capabilities of this remarkable technology and why so many law enforcement agencies are using facial recognition as a layer of safety and security for their officers in the field.

Regards,

Paul

Paul Sibek

FACEFIRST

www.facefirst.com
15821 Ventura Boulevard, Suite 425
Encino, CA 91436

From:	William Tyree
Sent:	Wednesday, February 14, 2018 10:47 AM
To:	Purchasing
Subject:	xxxxx, here's a new law enforcement face recognition study

Hi xxxxx,

How many hours do your patrol officers spend identifying suspects in the field?

The FaceFirst team just created a new whitepaper that shows how face recognition:

- Saves law enforcement departments up to 100,000 hours by fully automating the identification process in the field
- Minimizes false arrests
- Provides officers with an added layer of safety
- Protects departments, prisons and jails

You can download it for free here. Download Whitepaper.

Would you be interested in getting a demo demonstrating how face recognition can help Las Vegas Metropolitan Police Department?

Best regards,

William Tyree | Chief Marketing Officer
FaceFirst, Inc
www.facefirst.com

To stop receiving occasional educational content you can unsubscribe from email communications.

1

The Growing Role of
Face Recognition
in Law Enforcement

FACEFIRST

CONTENTS

FACE RECOGNITION:
WHAT IT IS, AND WHAT IT ISN'T

Since the invention of face recognition in the 1960s, the promise of its role in law enforcement has sparked fascination for public safety officials, journalists and especially Hollywood filmmakers. Films like 2002's Minority Report helped spark the imagination of face recognition as a potential crime prevention and crime solving tool.[1] Much, but not all, of what was predicted decades ago has become possible.

Once used only by the military and public safety officials, the technology has become mainstream, appearing in the iPhone, Facebook and elsewhere. It is also used by hundreds of law enforcement agencies. Still, confusion remains about how exactly it can be used by law enforcement, and what its limitations are.

What Face Recognition Can Do

- Identify a person with over 99% accuracy from mugshots, live video footage or archived footage

- Help patrol officers make instant IDs in the field

- Alert stations and courthouses about the presence of unwanted or potentially dangerous individuals in sensitive areas

- Quickly match an image against vast databases of mugshots from multiple state, local, federal and international agencies

What Face Recognition Can't Do

- Predict that a person will commit a crime

- Predict that a person will become a criminal

- Deliver accurate matches in darkness

- 100% positively identify individuals. The FBI advises use of face recognition "as an investigative lead, not as a means of positive identification."[2]

FACEFIRST

BRIEF HISTORY OF FACE RECOGNITION

Face recognition accuracy and performance speeds are now effective for even the most robust mobile, surveillance, access control and forensic use cases, but it has taken decades of development to get to this point.

Here are the major milestones:

1960s	First manual measurements created using electromagnetic pulses[3]
1970s	21 points of measurements agreed upon by major researchers
1988	100 points of measurement applied using linear algebra
1991	First crude automatic face detection from images
1993	Defense Advanced Research Projects Agency (DARPA) created the first basic database of facial images
2002	A database of 856 people was used at Super Bowl XXXV. The experiment failed
2003	DARPA database upgraded to 24-bit color facial images
2004	National Institute of Standards and Technology (NIST) test created
2009	Pinellas County Sherriff's Office creates forensic database
2010	Facebook begins implementing face recognition to auto-tag images
2011	Panama Airport installs first face recognition surveillance system[4]
2011	Body of Osama Bin Laden positively identified via face recognition
2012	16,000 points of measurement used in Cognitec algorithm
2013	FaceFirst achieves effective mobile deployment speeds
2014	ARJIS deploys cross-agency system in southern California
2016	U.S. deploys exit face recognition at Atlanta Airport
2017	150,000 points of measurement used in FaceFirst algorithm
2017	iPhone X breaks selling records with face recognition access control

FOUR COMMON USES OF FACE RECOGNITION IN LAW ENFORCEMENT

Face recognition technology can be used by many different types of law enforcement personnel across four major categories.

Forensic

Typically used by investigators, forensic face recognition software systems can recognize individuals from mugshots and surveillance footage, typically after a crime has been committed. These were the first types of face recognition systems to be used in law enforcement.

> Face recognition matches a smartphone photo against a database of known criminals and suspects

Mobile

Typically used by patrol officers, mobile face recognition enables police to take a photo with a smartphone and match it against a vast database of known criminals and suspects. The primary objective of mobile systems is to instantly identify individuals in the field and gain immediate access to outstanding warrants and prior criminal history, if any.

Surveillance

Typically used by stations and courthouses, face recognition surveillance attempts to identify known criminals the moment they enter an area and alerts command center staff or patrol officers about their presence.

Access Control

Face recognition can be used to enable entry into sensitive areas, such a station's back offices. The technology is typically used as a secondary method of access, with a badge or code also being required as well.

Quality data – mugshots, names, criminal history and more – is essential to all four major use cases. Ideally, a fully managed and curated criminal intelligence database should allow departments to publish and subscribe to data from other local and state partners, as well as networks such as COPLINK.

CAN FACE RECOGNITION MAKE CRIMINAL INTELLIGENCE ACTIONABLE FOR PATROL OFFICERS?

Over the past two decades, the law enforcement community has gained access to unprecedented quantities of digitized criminal intelligence data. When it comes to the process of positively identifying individuals, however, patrol officers have not benefitted from the data boom nearly as much as their counterparts in command centers. Mobile devices and in-car computers have helped, but those technologies by themselves aren't able to empower officers to make critical split-second decisions based on actionable, real-time data.

When confronted with individuals that don't present valid identification, present false information, don't speak a common language or are unconscious, patrol officers must resort to manual searches, coordination with station personnel, and even trips to the station. Resource-strapped departments sometimes have to make hard choices and move on to a higher priority call without ever establishing ID.

> **Mobile devices and in-car computers by themselves aren't able to empower officers to make critical split-second decisions**

Over the past four years, real time mobile face recognition platforms have made criminal intelligence data truly actionable. Such platforms allow officer to:

- Establish ID from a safe distance

- Minimize false arrests, preventing lawsuits and bad press

- Surface outstanding warrants or prior arrest records

- ID persons that are unconscious or dead

FACEFIRST

HOW MOBILE FACIAL RECOGNITION WORKS

STEP 1   Officers download an app to their smartphone.

STEP 2   Patrol officers snap a photo of any individual using their phone camera. When using a high-quality application sensitive enough to estimate depth, no special 3-D camera is required.

STEP 3   The image is automatically and instantly matched against a large database of photos at speeds upward of 25 million per second.

> Database profile matches are returned within five seconds, along with outstanding warrants, past arrests and more

STEP 4   Database profile matches are returned within five seconds, along with actionable information including outstanding warrants, past arrests and more.

Additionally, the officer may choose to add notes to an existing profile – including new photos showing changes in appearance such as tattoos or piercings – from the phone application.

If the individual is not in the database, and department protocols allow, the officer may choose to enroll the image as a new profile.

THE ECONOMICS OF MOBILE FACIAL RECOGNITION

Facial recognition provides law enforcement departments with a number of transformative benefits including:

Identity Acceleration: Face recognition enables patrol officers to accurately identify individuals in seconds, not hours, complete with actionable intelligence including outstanding warrants, past arrest history and other relevant details.

Force Multiplication: In some departments, as much as 10% of an officer's shift is spent manually establishing identities. Commonly replaced activities include:

- questioning and notetaking

- manual identity searches

- cross-department records requests, including mugshots

- transportation and fingerprinting

By instantly identifying suspects, face recognition empowers officers to effectively spend up to 200 extra hours per year in the field, or the equivalent in fully loaded average patrol officer salary of $7,700 (based on an average salary of $55,000/year, plus 40% in benefits).[5] For a force of 500 sworn officers this can equal as much as 100,000 extra hours a year, or nearly $3.85M in total fully loaded salary costs. The time savings offers the benefit of having more officers on patrol, without having to allocate additional salary costs.

Minimizing Legal Costs from False Arrests: Face recognition can prevent suspects from using the identity of innocent citizens, and can therefore prevent law-abiding civilians from being falsely arrested.

False arrests typically result in bad press for departments. But in addition to being embarrassing, they can result in expensive legal settlements and even cost officers their jobs. Consider:

- Press impact – Tens of thousands of press mentions per incident

- Price per incarcerated hour – $7,700[6]

- Settlement fees – Up to $625,000[7]

■ Total expenses related to a false arrest – Potentially millions, including legal fees, settlements, public relations and other factors.

Public Assistance & De-escalation: Given access to state health and welfare institutional data, face recognition can help notify officers of known mental health issues so individuals can be directed to get the help they need.

10%
PERCENTAGE OF AN OFFICER'S SHIFT SPENT MANUALLY ESTABLISHING IDENTITIES

100,000
EXTRA HOURS/YEAR GAINED WITH FORCE OF FIVE HUNDRED OFFICERS

$7,700
PRICE PER INCARCERATED HOUR FOR A FALSE ARREST

$3.95M
SALARY SAVED PER YEAR WITH A FORCE OF 500 OFFICERS

$625,000
MAXIMUM SETTLEMENT FEES INCURRED WITH EACH FALSE ARREST

FACEFIRST

CASE STUDY: THE AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM (ARJIS)

ABOUT ARJIS

The Automated Regional Justice Information (ARJIS) was created as a Joint Powers Agency to share information among justice agencies throughout San Diego and Imperial Counties, California. ARJIS has evolved into a complex criminal justice enterprise network used by 80+ local, state, and federal agencies. ARJIS is responsible for major public safety initiatives, including wireless access to photos, warrants, and other critical data in the field, crime analysis tools evaluation, and an enterprise system of applications that help solve crimes.

The Challenge

- Radically reduce the process of identifying persons of interest in the field

- Ensure dangerous fugitives don't slip through the cracks

- Break through language barriers during the ID process

- Minimize false arrests

The Solution

- Mobile face recognition

- Biometric enrollment platform

The Results

- 12,000+ police actions resulting from field matches and counting

- Reduces field investigation process from hours to seconds, saving officers hours of productivity each week

- Expansion to dozens of local, state and federal agencies including San Diego PD, FBI, DEA, ATF, CBP, DOJ and U.S. Marshalls[8]

- Zero legal or privacy complaints from the community

STUDY DETAILS

After a 35-year career in peace officer service, ARJIS analyst Lloyd Muenzer began analyzing technological solutions to help facilitate data sharing among all the law enforcement agencies in San Diego County. His first task was monumental: he needed to find a way to help patrol officers positively identify suspects in the field.

When stopping persons of interest, patrol officers often met individuals claiming not to have identification. Verifying identity in such scenarios required verbal descriptions to be matched against a database manually, which was time-consuming and often imprecise. The challenge was compounded when persons of interest did not speak English.

"There was really no positive identification in the field, per se," said Muenzer. "Traditionally, the officer would ask the person's name, date of birth, they would go through dispatch over the radio and ask them to run the person to see if there is a record somewhere. They'd literally have to do that by voice."

> ## "I get nothing but positive feedback. Literally everybody wants it!"
>
> **— Lloyd Muenzner**
> **Analyst, ARJIS**

To solve this problem, Muenzer began conducting a market analysis of face recognition vendors. While evaluating facial recognition solutions, he came across FaceFirst. After implementing a FaceFirst pilot program, Muenzer was instantly impressed. "People were having really, really good success with FaceFirst. I realized then how much potential this technology has."

With the goal of minimizing friction during the training process, an intuitive user interface was important to Muenzer. "The application is like anything else that you download on your phone. It's very, very intuitive to start with. Generally speaking, you can figure it out on your own." The response from officers has been unanimously positive. "I get nothing but positive feedback. Literally everybody wants it!"

For Muenzer, it was also important to find a solution that was CJIS compatible and could help protect privacy. "That's important because you really have to have con-

trol over [biometric] data. Mostly because we're protecting privacy rights for people out there and we have to make sure it's secure." FaceFirst is private by design, and has made it easy for ARJIS to maintain CJIS compliance and ensure that data is secure at all times. As a result, ARJIS hasn't received a single privacy complaint from the community.

FaceFirst has also helped Muenzer maintain checks and balances. "I get an email every time someone takes a picture of someone and the match percent [that's predicted] is a 90% match or better. And I check those daily to make sure those pictures are matching up. They almost always do."

After initial successes, ARJIS expanded the FaceFirst solution across dozens of departments, including local and state police, FBI, DEA, ATF and DOJ.

PLATFORM PERFORMANCE

Database Performance

FaceFirst can search and match against 25 million faces per second.

Alerting Speed

Patrol officers receive alerts in the field within 5 seconds on Android and iOS smartphones and tablets.

Points of Reference

FaceFirst measures roughly 150,000 points of reference on a face when establishing a person's identity.

Artificial Intelligence

When using biometric surveillance to protect departments, the FaceFirst algorithm utilizes machine learning techniques to determine the best face across hundreds or thousands of video frames. Factors such as face angle, lighting, expression, sharpness and others are all calculated, considered and processed at 30 frames per second.

25 MILLION
NUMBER OF FACES SEARCHED AND MATCHED PER SECOND

5 SECONDS IT TAKES TO ALERT PATROL OFFICERS WHEN THERE IS A MATCH

30 USED TO DETERMINE THE BEST FACE FOR MATCHING
FRAMES PER SECOND

150,000 FACIAL POINTS OF REFERENCE USED IN ESTABLISHING A PERSON'S IDENTITY

SECURITY AND COMPLIANCE

Face recognition platforms should be designed from the ground up to make protecting privacy a top priority. In its report regarding the commercial use of facial recognition technology, the Government Accountability Office (GAO) noted that facial recognition technology is actually less intrusive than traditional video surveillance, in that facial recognition technology only captures biometric information.[9] Here are some additional steps FaceFirst takes to ensure privacy, security and compliance:

Anti-profiling:

The FaceFirst system is designed to prevent utilizing the platform for any type of profiling by race, age, gender or national origin.

Encryption & Data Breach Precautions:

Image data is encrypted both at rest and during transmission. Biometric templates stored within the FaceFirst system cannot be converted back into a face image in the case of a data breach.

Data Purging:

Surveillance data is automatically purged at regular intervals to protect privacy.

> **Facial recognition technology is less intrusive than traditional video surveillance**
>
> — Government Accountability Office

Checks and Balances:

Role hierarchies ensure that only authorized individuals have the ability to approve and view enrollment images within the FaceFirst system.

CJIS Compatible:

FaceFirst is easily adaptable to changing rules and policies, and has a record of proven compliance across dozens of agencies.

SOURCES

1. Face Recognition Makes the Leap from Sci-Fi, 2011, *New York Times,* http://www.nytimes.com/2011/11/13/business/face-recognition-moves-from-sci-fi-to-social-media.html

2. Statement Before the House Committee on Oversight and Government Reform, 2017, FBI, https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology

3. How Facial Recognition Technology Came to Be, 2014, *Boston Globe,* https://www.bostonglobe.com/ideas/2014/11/23/facial-recognition-technology-goes-way-back/CkWaxzozvFcveQ7kvdLHGI/story.html

4. A Brief History of Face Recognition, 2017, *FaceFirst,* https://www.facefirst.com/blog/brief-history-of-face-recognition-software/

5. Entry Level Police Officer Salary in the United States, 2017, https://www.ziprecruiter.com/s/entry-level-police-officer-salary

6. AT & CT v. City of NY, a 17-hour wrongful detention resulted in an $80K settlement, 2015, http://mjrlaw-ny.com/lawyer/blog_category/False-Arrest-Stop-and-Frisk

7. Madison County Sherriff's Department Settles Revenge Beatdown Lawsuit, 2014, Al.com, http://www.al.com/news/index.ssf/2014/07/madison_county_sheriff_settles.html

8. Face Recognition and Law Enforcement Webinar, 2017, FaceFirst/ARJIS, https://www.facefirst.com/webinar-facial-recognition-sweeping-law-enforcement/

9. Face Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, 2015, *Government Accountability Office (GAO)* https://www.gao.gov/assets/680/671764.pdf

ABOUT FACEFIRST

FaceFirst is a global patented enterprise-grade facial recognition software platform designed to be scalable, fast and accurate while maintaining the highest levels of security and privacy*. We provide real-time threat notifications that prevent crime before it happens.
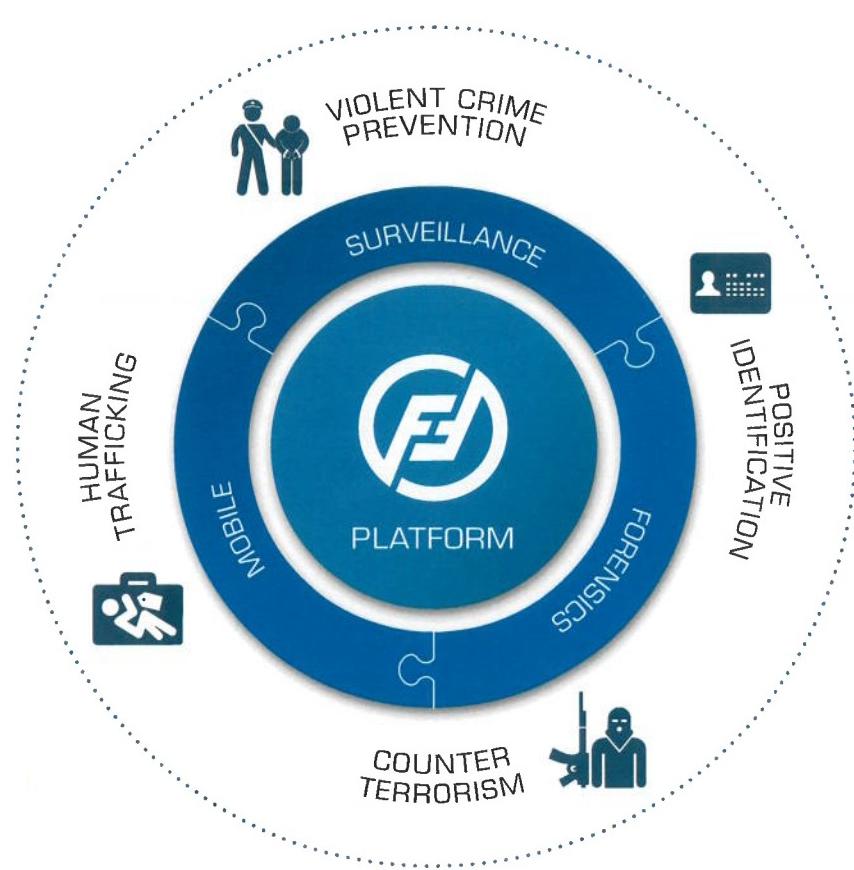
VISIT: FACEFIRST.COM

CALL: 818-540-9800